POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UM MODELO VOLTADO PARA UMA INSTITUIÇÃO DE ENSINO SUPERIOR

INFORMATION SECURITY POLICY: A MODEL BACKED TO AN INSTITUTION OF HIGHER EDUCATION

Ione Beatriz Pereira de Oliveira[1], Walter Costa Almeida Figueiredo[2], Ana Carolina Cintra Faria[3]
1 Aluna de Iniciação Científica e do Curso de Sistemas de Informação do UNIDESC
2 Professor do Curso de Sistemas de Informação e Orientador do Projeto de Iniciação Científica do UNIDESC.
3 Professora do Curso de Sistemas de Informação e Co-Orientadora do Projeto de Iniciação Científica do UNIDESC.

RESUMO
A tecnologia está cada vez mais presente dentro das empresas como um ativo facilitador na busca e no compartilhamento de informações, por isso é necessário saber protegê-las, pois elas têm um grande valor no âmbito profissional. A partir dessa visão, desenvolveu-se esse trabalho com o objetivo de criar uma Política de Segurança da Informação para a instituição de ensino superior. A necessidade da criação da política se deu a partir do resultado de uma pesquisa quantitativa em que foi possível identificar o baixo nível de maturidade por parte dos funcionários da instituição, no que diz respeito a segurança da informação. A política tem como objetivo proteger os ativos de tecnologia da instituição, determinando normas a serem seguidas para reduzir os incidentes resultantes da falta de proteção.
Palavras–Chave: Tecnologia; Política de Segurança da Informação; Proteção.

Abstract
Technology is increasingly present within companies as an active facilitator in the search and sharing of information, so it is necessary to know how to protect them, since they have a great value in the professional scope. Based on this vision, this work was developed with the objective of creating an Information Security Policy for use in an institution of higher education. The need to create the policy was based on the results of a quantitative research in which it was possible to identify the low level of information security maturity.
The policy aims to protect the institution's technology assets, setting standards to be followed to reduce incidents resulting from lack of protection.
Keywords: Technology; Information Security Policy; Protection.

Contato: ionebeatriz.po@gmail.com, anacarolina.cintrafaria@gmail.com, walter.fig@gmail.com

INTRODUÇÃO

A informação está presente em todos os lugares, principalmente nas organizações, incluindo as instituições de ensino, que são ambientes voltados para a produção de conteúdo visando o compartilhamento e disseminação de conhecimento. Por isso, é notória a importância de protegê-la, para que se possa ter acesso a ela no momento em que houver necessidade, porém sabe-se que preservar informações não é uma tarefa fácil.

Um dos meios de proteger informações em uma organização é fazendo uma implantação de uma Política de Segurança da Informação (PSI). A implantação de uma PSI é um processo que demanda padronização, estabelecimento de limites e envolve todos os setores, principalmente os associados a tomada de decisão na organização. Martins e Santos (2005), ao elaborar uma metodologia para implantação de um sistema de gestão de segurança da informação, já mapearam que o documento deverá apresentar algumas características, conforme especifica a ISO/ IEC17799:

(i) ser aprovada pela diretoria, divulgada e publicada de forma ampla para todos os colaboradores; (ii) ser revisada regularmente, com garantia de que, em caso de alteração, ela seja revista; (iii) estar em conformidade com a legislação e cláusulas contratuais; (iv) deve definir as responsabilidades gerais e específicas; (v) deve dispor as consequências das violações.

A necessidade de explorar esse tema é de extrema importância, pois a informação deve ser vista como um dos principais tipos de patrimônio existente dentro das organizações, por isso é considerável que ela seja preservada de qualquer tipo de evento que possa vir a danificá-la, entretanto, nos tempos atuais são poucos os investimentos em segurança da informação (SI) no ambiente acadêmico pois várias instituições de ensino superior carecem de políticas de segurança da informação, tendo em vista as constantes notícias de ataques, quebras de páginas e falhas na rede que são veiculadas na internet todos os dias.

O interesse pelo tema surgiu conforme exposto acima, da necessidade de difundir os benefícios trazidos pela segurança da informação, e seu caráter imprescindível em qualquer organização. No sentido de conferir efetividade ao projeto, adotou-se como base os princípios básicos da segurança da informação que segundo a ISO/IEC 17799:2005 são Confidencialidade, Integridade, Disponibilidade, Autenticidade, Irretratabilidade e Conformidade.

De acordo com a ISO IEC 27002, que é uma norma reconhecida mundialmente como referência em segurança da informação, as políticas de segurança da informação visam prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis de regulamentações relevantes.

O presente trabalho surgiu da necessidade de proteger informações no âmbito institucional, a fim de conferir as informações utilizadas em cada setor da instituição, um grau de acessibilidade e disponibilidade das informações, resguardando e protegendo o conhecimento produzido na esfera acadêmica.

Em um primeiro momento foi possível verificar o nível de maturidade da SI na instituição (IES) e com o resultado desse estudo, foi constatada a necessidade de desenvolver uma PSI para a IES, uma vez que foi comprovada a baixa maturescência da SI na instituição.

Dessa forma, o princípio que estruturou a pesquisa foi a importância do uso correto da TI e da manipulação das informações dentro do Centro Universitário de Desenvolvimento do Centro-Oeste (UNIDESC), de forma segura.

Enquanto objetivo geral, com essa pesquisa pretende-se desenvolver uma política de segurança da informação baseada na ISO 27001/2005 e em uma metodologia que propõe a implantação de políticas de segurança da informação a fim de proteger informações que precisam ser compartilhadas no âmbito de uma instituição de ensino superior do entorno sul de Brasília. No que se refere aos objetivos específicos, pretende-se: i) Realizar uma revisão de literatura sobre os conteúdos essenciais pré-definidos: segurança da informação, ISO 27001/2005, mapeamento de processos, segurança da informação no âmbito de instituições de ensino superior; ii) Avaliar em conjunto com a direção da IES os níveis hierárquicos e de permissão para as informações, a fim de desenhar o escopo da política.

OBJETIVOS

Objetivo geral: Desenvolver uma política de segurança da informação baseada na ISO 27001/2005 e em uma metodologia que propõe a implantação de políticas de segurança da informação a fim de proteger informações que precisam ser compartilhadas no âmbito de uma instituição de ensino superior do entorno sul de Brasília.

Objetivos específicos:

- Mapear os processos acadêmicos e administrativos da instituição de ensino superior.
- Realizar uma revisão de literatura nos últimos 10 anos sobre os conteúdos essenciais pré-definidos: segurança da informação, ISO 27001/2005, mapeamento de processos, segurança da informação no âmbito de instituições de ensino superior.
- Avaliar em conjunto com a direção da ies os setores que carecem de urgência na elaboração da política de segurança da informação e priorizá-los para a elaboração da mesma.

REVISÃO DA LITERATURA

Segurança da Informação

A informação é a principal arma estratégica nas empresas, por isso é considerada um recurso de muita importância. “A segurança da informação de uma empresa garante, em muitos casos, a continuidade de negócio, incrementa a estabilidade e permite que as pessoas e os bens estejam seguros de ameaças e perigos.” (BLUEPHOENIX, 2008)

Em toda parte, é possível encontrar informação, em documentos eletrônicos ou impressos, em vídeos, imagens, em

servidores de arquivos e bancos de dados por exemplo. Entretanto, o valor da informação muitas vezes só é reconhecido quando ela é violada, perdida ou roubada e isso leva as empresas a arcar com os prejuízos de se ter informações danificadas e geralmente os custos são altos. "Custo nesta citação significa apurar o valor das perdas tanto em dinheiro quanto na reputação da organização, na confiança e em outros valores que a organização mantém como princípio de sua missão como empresa." (DAVIS, 1997 APUD BLUEPHOENIX, 2008).

Para que seja possível manter a informação segura, é necessário que as empresas implantem um projeto de segurança da informação avaliando e estabelecendo procedimentos, mecanismos e níveis de segurança.

Os mecanismos de segurança devem garantir que cada funcionário tenha uma única identidade no sistema por exemplo, isso pode ser feito através de uma autenticação com login e senha no sistema da ies, focando em um dos princípios de segurança da informação que é a autenticidade pois ele "determina se alguém (ou algo) é, de fato, quem (ou o que) afirma ser." Barcellos e Marinho, (200?).

Já os níveis de segurança devem assegurar que cada funcionário deverá ter acesso apenas ao que lhe cabe, por exemplo, um professor da ies, só deve ter acesso a informações que estejam no seu escopo de trabalho e não poderá acessar dados ou informações sobre outros departamentos que ele não atua.

ISO/IEC 27001:2005

A ISO/IEC 27001 é uma norma de gestão de segurança da informação que descreve como colocar em prática um sistema de gestão de segurança da informação.

A norma tem como princípio geral a adoção pelas instituições, de um conjunto de requisitos e processos com o objetivo de gerenciar adequadamente o risco das instituições, ela tem sido melhorada e atualizada ao longo dos anos e a origem dela vem de um documento publicado em 1992 pelo governo britânico.

Segundo Galegale e Cantón (2007-2008), "a norma NBR ISO/IEC 27001:2005 é a revisão da norma BS 7799-2:2002, um padrão britânico que trata da definição de requisitos para um Sistema de Gestão de Segurança da Informação."

Ao longo dos anos, muitos profissionais contribuíram para que ela evoluísse e ganhasse um escopo maduro que certamente irá continuar a evoluir.

Segundo o Portal Informativo:

"Milhões de entidades no mundo utilizam as práticas documentadas no Standard e usufruem dos benefícios da sua adopção, sendo que, as entidades que assim o desejem podem também certificarem-se, demonstrando assim de forma idónea que cumprem os requisitos e os processos constantes na norma."

Mapeamento de Processos

O mapeamento de processos é definido na pesquisa de Hunt (1996) como "uma ferramenta gerencial analítica e de comunicação que tem a intenção de ajudar a melhorar os processos existentes ou de implantar uma nova estrutura voltada para processos".

Com uma análise detalhada dos processos, é possível sugerir uma melhor administração dos mesmos através da política de segurança que será elaborada.

O mapeamento dos processos na instituição, será feito verificando a localização e quantidade de ativos de TI, quantidade de usuários, quantidade de sistemas utilizados, também será verificado o fluxo de interação dos usuários entre os sistemas existentes para que se possa definir o que é necessário para montar o escopo da PSI, usando esses pontos como delimitadores de escopo.

Segurança da informação no âmbito de instituições de ensino superior

Conforme especifica a ISO/IEC 17799:2005 "garantir segurança da informação significa proteger a informação de vários tipos de ameaça para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades do negócio."

Em instituições de ensino superior, existem dois tipos de usuários, o primeiro é o funcionário, que trabalha na instituição e o segundo é o aluno, que frequenta a instituição, participa das aulas e desenvolve trabalhos e nesses momentos, ambos estão utilizando os recursos disponibilizados pela instituição.

Conforme exposto anteriormente, a Política de Segurança da Informação é um documento que tem como objetivo estabelecer algumas recomendações e procedimentos visando prevenir os incidentes de segurança dentro de uma organização, uma PSI voltada para uma instituição de ensino, deve ser criada de forma a estabelecer normas a serem seguidas por todos os usuários, no que diz respeito aos ativos de informática, de modo que todos os envolvidos tenham consciência que é importante proteger e utilizar com prudência os recursos de TI na instituição.

Segundo Martins e Santos, (2005), "a Política de Segurança deverá apresentar algumas características, conforme especifica a ISO/ IEC17799: (i) ser aprovada pela diretoria, divulgada e publicada de forma ampla para todos os colaboradores; (ii) ser revisada regularmente, com garantia de que, em caso de alteração, ela seja revista; (iii) estar em conformidade com a legislação e cláusulas contratuais; (iv) deve definir as responsabilidades gerais e específicas; (v) deve dispor as conseqüências das violações."

METODOLOGIA

Quanto ao objetivo é possível caracterizar esta pesquisa como sendo de natureza básica e de abordagem qualitativa, que segundo Goldenberg (1997) não se preocupa com representatividade numérica, mas, sim, com o aprofundamento da compreensão de um grupo social, de uma organização, etc. Os pesquisadores que adotam a abordagem qualitativa opõem-se ao pressuposto que defende um modelo único de pesquisa para todas as ciências, já que as ciências sociais têm sua especificidade, o que pressupõe uma metodologia própria (GOLDENBERG, 1997, p. 34).

Quanto aos procedimentos técnicos, pode-se caracterizar este estudo como sendo uma pesquisa bibliográfica e exploratória, pois [...] foi feita a partir do levantamento de referências teóricas já analisadas, e publicadas por meios escritos e eletrônicos, como livros, artigos científicos, páginas de web sites (FONSECA, 2002, p. 32). Além de explorar um universo pré-definido e realizar intervenções sobre ele.

No que se refere a abordagem do problema o método utilizado para esta pesquisa foi quali-quantitativo, ou método misto, bastante utilizado em estudos exploratórios, como é o caso da elaboração desta política, tendo em vista que estes estudos se inicial com pouco conhecimento inicial sobre o problema investigado e suas fronteiras.

O processo de validação das condições de aplicação da pesquisa de predominância quali-quantitativa possibilita que o desenvolvimento de um design de pesquisa enquanto mapa de navegação favoreça a avaliação por critérios de cientificidade e aderência ao problema como percebido por seu interlocutor (decisor). A primeira etapa denominada validação e a segunda, legitimação. O design da pesquisa deve explicitar os tipos de escalas a serem utilizadas em cada uma de suas etapas e a forma de sua transformação em escalas cardinais, se for esse o caso. (ROY, 1993; MISER, 1993; ORAL E KETANY, 1993; LAUNDRY, 1995 apud ENSSLIN, 2008, p.10).

Deste modo, o método misto foi utilizado para a elaboração de um questionário (instrumento de coleta de dados), com 7 (sete) questões objetivas acerca de mecanismos e processos basilares de segurança da informação dentro de uma IES. As respostas traçaram um perfil quanto ao nível de conhecimento (maturidade) dos funcionários tanto administrativos quanto docentes sobre o tema. O link do questionário, elaborado na plataforma SurveyMonkey, foi enviado no formato digital aos colaboradores. Esta pesquisa foi submetida ao comitê de ética em pesquisa com seres humanos das Faculdades Promove de Brasília e aprovada sob o número do parecer consubstanciado: 2.401.978. A aplicação da pesquisa ocorreu no período de outubro a novembro de 2017.

DESCRIÇÃO DO CASO

A instituição de ensino superior Centro Universitário de Desenvolvimento do

Centro-Oeste não possui uma Política de Segurança da Informação (PSI), algo que é imprescindível para manter segura a infraestrutura e as aplicações de tecnologia da instituição, por isso a iniciativa do trabalho foi criar a PSI com base no resultado da pesquisa que evidencia a necessidade da política.

Visando minimizar os riscos que o Unidesc corre por não seguir uma norma, a PSI reuniu todos os usuários de serviços de tecnologia da instituição. Para isso, o primeiro passo na busca de uma solução para a situação, foi a identificação do que deve ser protegido, incluindo o levantamento dos ativos que estão envolvidos, e de quem é necessário proteger, qual a possibilidade real de ameaças, e por fim, um levantamento de dificuldades e sugestões de medidas de proteção e prevenção.

Segundo Martins e Santos, (2005), "a implantação da gestão de segurança da informação começa pela definição de quais dos itens especificados em cada padrão devem ser implementados na organização. Em outras palavras, é necessário definir se os itens do padrão estão adequados às características da organização."

A política foi elaborada e deverá ser aprovada pelos gestores da instituição, para que possa ser de fato implantada, depois disso, deverá ser divulgada a todos os colaboradores e acadêmicos da instituição.

A PSI elaborada tem como características principais, os seguintes aspectos:

Propriedade da informação - isso diz respeito a definir um responsável pela informação, ou seja, definir os níveis de acesso a todo tipo de informação que trafega na ies.

Controle de acesso - essa característica se refere a privilégios de acesso, toda solicitação de acesso a qualquer sistema de informação, deve ser registrada.

Gerência de usuários e senhas - cada usuário e senha deve ser individual e as senhas devem ter um nível de confiabilidade forte. Cada usuário deverá ser responsável por sua senha.

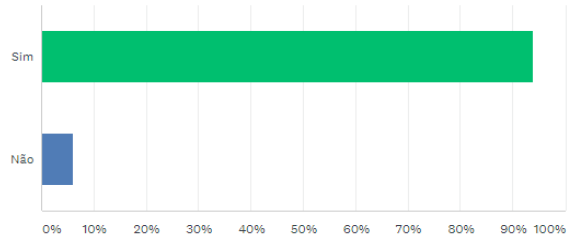
Segurança Física - qualquer tipo de acesso ao CPD da ies deve ser feito mediante autorização pelos responsáveis por monitorar o ambiente e os equipamentos que estão no local.

RESULTADOS

O estudo envolveu 152 funcionários, sendo eles colaboradores da área administrativa e área docente. Os e-mails foram enviados para todos e durante um período de 30 dias, foram recebidas 33 respostas.

Os mecanismos de segurança da informação só serão eficazes se as pessoas contribuírem para isso fazendo o uso correto e eficaz dos recursos que estão a seu dispor. Com a aplicação do questionário foi possível verificar que 93,94% dos usuários diz saber o que quer dizer segurança da informação, Gráfico 1. O que é importante, pois segundo Fontes (2008), proteger a informação é considerar as pessoas um elemento vital. As pessoas fazem a organização. As pessoas fazem acontecer a segurança da informação.

Gráfico 1: Percentual de respostas sobre o conhecimento sobre o conceito de segurança da informação

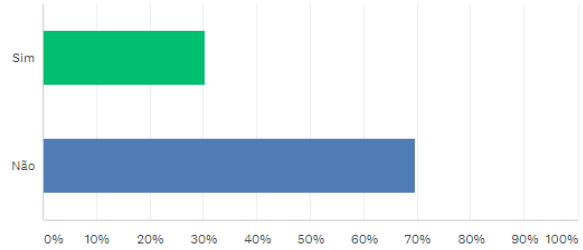


Fonte: Próprio autor

Na questão seguinte, foi possível notar que o número de usuários que foram vítimas de falhas de segurança da informação na instituição foi de 30,30%, ou seja, de um total de 33 pessoas que responderam, 10 tiveram informações de seus computadores ou dispositivos portáteis roubadas ou corrompidas de alguma forma, por isso, pode-se afirmar que possivelmente os dispositivos desses usuários foram infectados com algum tipo de vírus[1].

[1] Um vírus de computador é um programa ou pedaço de código que é carregado ao seu computador sem seu conhecimento ou permissão. Alguns vírus são meramente irritantes, mas a maioria dos vírus são destrutivos e designados a infectar e controlar sistemas vulneráveis. Um vírus pode se alastrar a vários computadores e redes ao criar cópias dele mesmo, assim como um vírus biológico passa de uma pessoa

Gráfico 2: Percentual de respostas sobre a quantidade de usuários que já foram vítimas de alguma falha de segurança de informação na instituição

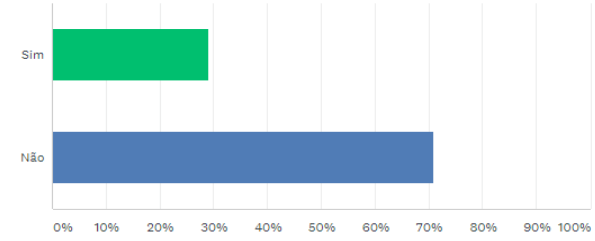


Fonte: Próprio autor

Com isso, também foi possível constatar que a baixa maturescência da segurança da informação na instituição é conseqüência da falta de padrões e normas já que 70% dos usuários afirmaram que na instituição não existia nenhum documento de processos e procedimentos de segurança da informação conforme mostra o gráfico abaixo.

Entretanto, 29,9% dos usuários dizem que esse documento existe, mas a falha no processo de conscientização da segurança da informação é evidente, pois, o procedimento correto seria que todos os colaboradores tivessem acesso a ela.

Gráfico 3: Percentual de respostas sobre o conhecimento dos usuários acerca da existência de alguma documentação dos processos e procedimentos referentes aos recursos de informação na instituição



Fonte: Próprio autor

A SI é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. (LYRA. 2008 apud CASTILHO e FONTE, 2012).

A Política de Segurança da Informação é um conjunto de normas que definem como os ativos de tecnologia da empresa devem ser protegidos, fazendo com que os usuários tenham acesso apenas ao que for necessário, explicitando o que é permitido fazer ou não.

As normas descritas no decorrer devem sofrer alterações sempre que necessário, sendo que qualquer modificação deve ser registrada e divulgada, se existir necessidade de mudança no ambiente deve-se solicitar com tempo hábil para que as providências necessárias sejam tomadas. (SPANCESKI, 2004)

A implantação de uma Política de Segurança da Informação é um processo que demanda padronização, estabelecimento de limites e envolve todos os setores, principalmente os associados à tomada de decisão na organização. Da necessidade de difundir os benefícios trazidos pela segurança da informação, e seu caráter imprescindível em qualquer organização. Para que o projeto fosse efetivo, foram seguidos os princípios básicos da segurança da informação que, segundo a ISO/IEC 17799:2005, são:

Confidencialidade: propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

Integridade: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (Corrente, intermediária e permanente). O ciclo de vida da informação orgânica - criada em ambiente organizacional - segue as três fases do ciclo de vida dos documentos de arquivos; conforme preceitua os canadenses da Universidade do Quebec (Canadá): Carol Couture e Jean Yves Rousseau, no livro Os Fundamentos da Disciplina Arquivística.

Disponibilidade: propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

Autenticidade: propriedade que garante que a informação é proveniente da fonte

para a outra. (Avast – Vírus de Computador, 2017). <https://www.avast.com/pt-br/c-computer-virus>. Acesso em 06 de novembro de 2017.

anunciada e que não foi alvo de mutações ao longo de um processo.

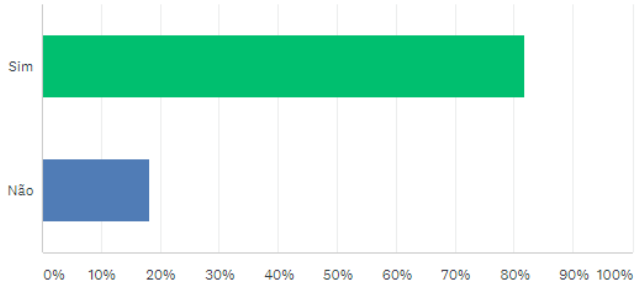
Irretratabilidade ou não repúdio: propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita.

Conformidade: propriedade que garante que o sistema deve seguir as leis e regulamentos associados a este tipo de processo.

O ambiente físico também deve ser considerado no processo de ações para prevenir as informações de ataques, dentro de uma organização existem departamentos que são classificados por cargos e hierarquias, por isso e cada usuário deve ter acesso aos locais que executam suas atividades, pois ali deve estar todo tipo de informação que só ele e os seus colegas de departamento podem acessar.

Na pesquisa, 81,82% dos respondentes disseram ter autorização de acesso físico aos ambientes que necessitam acessar para executar suas atividades profissionais na instituição e com isso é possível afirmar que a segurança no ambiente físico tem um bom nível de maturidade, mas ainda assim é muito importante transmitir para o usuário que as restrições de acesso a locais, sistemas, arquivos, mídias entre outros são para proteger as informações que estão armazenadas nesses locais, independente de serem em um ambiente físico ou virtual.

Gráfico 4: Percentual de respostas dos colaboradores sobre a autorização que eles possuem aos ambientes em que necessitam acessar (fisicamente) para desempenhar suas atividades profissionais na instituição

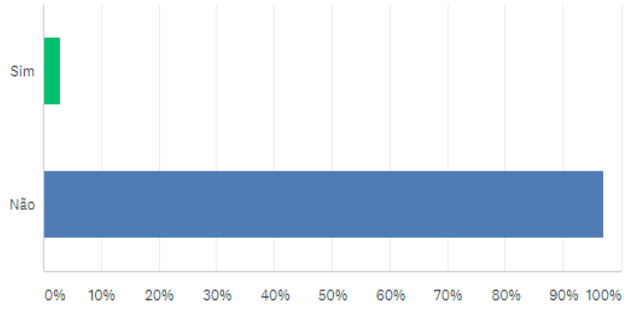


Fonte: Próprio autor

O ponto mais crítico da pesquisa se refere à conscientização do usuário visto que na instituição, 96,97% dos usuários nunca participaram de um processo de conscientização e treinamento em segurança da informação promovido pela instituição. Sabe-se que nenhuma instituição nasce com uma cultura formulada e que ao longo do tempo isso vai sendo construído com base no que foi almejado como cultura e com as ações que são executadas cotidianamente. Os pontos chaves para incluir algo na cultura organizacional são determinar e executar. Sendo importante e recomendável trabalhar no sentido de formar a cultura da segurança da informação em todos os usuários através de treinamentos, palestras ou workshops por exemplo.

Segundo Fontes (2008) a não existência de um processo de segurança da informação e manutenção de cultura em segurança da informação enfraquece a cadeia de valores para conseguirmos o nível adequado de proteção.

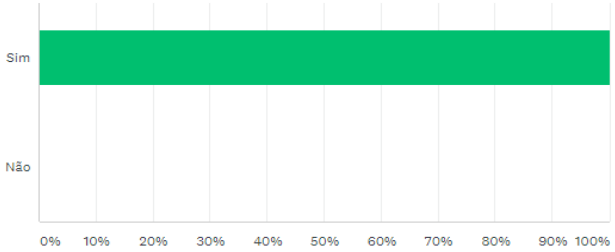
Gráfico 5: Percentual de respostas sobre a participação dos colaboradores em processos de conscientização e treinamentos em segurança da informação promovidos pela instituição



Fonte: Próprio autor

Um ponto positivo que a pesquisa evidenciou foi que parte do princípio de irretratabilidade que diz que o usuário não pode negar a autoria de acessos e modificações em informações está sendo seguido, pois 100% dos respondentes disseram que suas identificações nos sistemas da instituição são únicas e individuais.

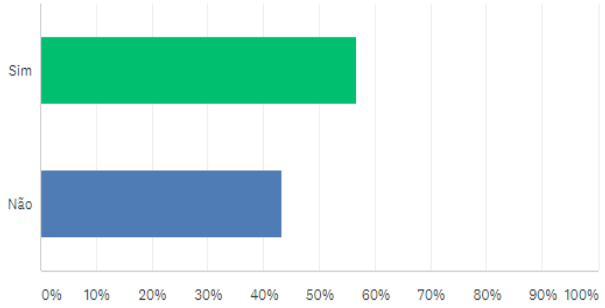
Gráfico 6: Percentual de respostas sobre a identificação dos usuários nos sistemas da instituição (e-mail, sistema acadêmico) com o intuito de avaliar se ela é única e individual



Fonte: Próprio autor

Porém, em outra questão ainda referente a irretratabilidade, 43,33% dos usuários disseram que a cadeia de caracteres que formam a sua identificação de usuário nesses sistemas, não possibilita fazer a ligação com os seus dados complementares e descritivos, o que torna falho o processo de identificação do usuário em caso de auditoria.

Gráfico 7: Percentual de respostas a respeito da cadeia de caracteres que formam a identificação dos usuários nos sistemas da instituição com o intuito de verificar se ela possibilita fazer a ligação com os dados complementares e descritivos dos usuários



Fonte: Próprio autor

Com base nesses resultados, foi possível organizar a elaboração da PSI. A ISO/IEC 27001:2005 - Tecnologia da informação - técnicas de segurança - sistemas de gerência da segurança da informação – requisitos foi escolhida para servir como base para a elaboração da política, pois se trata de uma norma que tem como objetivo detalhar como colocar em prática um sistema de gestão de segurança da informação. E a metodologia elaborada por Spancesk (2004) foi utilizada porque tem como foco a aplicação de uma PSI em uma instituição de ensino, o que tornou o estudo mais consistente, pois a aplicação da política tinha o mesmo contexto.

O desenvolvimento da PSI se deu com base nas seguintes fases: levantamento das informações, desenvolvimento do conteúdo político e das normas, elaboração dos procedimentos de SI e revisão, aprovação e implementação. (FERREIRA e ARAÚJO, 2008 apud CASTILHO e FONTE, 2012)

A política elaborada nesse trabalho tem como características principais, os seguintes aspectos.

Propriedade da informação: isso diz respeito a definir um responsável pela informação, ou seja, definir os níveis de acesso a todo tipo de informação que trafega na instituição.

Controle de acesso: essa característica se refere a privilégios de acesso, toda solicitação de acesso a qualquer sistema de informação, deve ser registrada.

Gerência de usuários e senhas: cada usuário e senha deve ser individual e as senhas devem ter um nível de confiabilidade forte. Cada usuário deverá ser responsável por sua senha.

Segurança Física: qualquer tipo de acesso ao CPD da instituição deve ser feito mediante autorização dos responsáveis pelo monitoramento do ambiente e dos equipamentos que estão no local.

A partir dos resultados obtidos, e o maior número de resposta ter se concentrado nos funcionários, a política foi elaborada para que os funcionários que se utilizam dos recursos informacionais da IES possam se orientar pela mesma. Após validação e implantação no corpo técnico administrativo, pretende-se colher os dados através do questionário com os alunos e docentes da IES.

CONSIDERAÇÕES FINAIS

Este trabalho se propôs a desenvolver uma política de segurança da informação baseada na ISO 27001/2005, e em uma metodologia que propõe a implantação de políticas de segurança da informação a fim de proteger informações que precisam ser

compartilhadas no âmbito de uma instituição de ensino superior do entorno sul de Brasília.

Para atingir o objetivo proposto foi elaborado um questionário e o nível de maturidade sobre o termo segurança da informação foi medido, a fim de que a política pudesse refletir ações e o contexto da ies.

No que se refere aos objetivos específicos, pretendeu-se:

i) Realizar uma revisão de literatura sobre os conteúdos essenciais pré-definidos: segurança da informação, ISO 27001/2005, mapeamento de processos, segurança da informação no âmbito de instituições de ensino superior: O estudo da literatura nos mostrou que investir no desenvolvimento de atividades voltadas para proteger a segurança da informação minimiza prejuízos sejam eles financeiros ou morais. Aplicar o uso de normas na instituição garante o aumento de credibilidade aos usuários que nesse caso além dos colaboradores, a instituição também tem como usuários os alunos.
ii) Avaliar em conjunto com a direção da IES os níveis hierárquicos e de permissão para as informações, a fim de desenhar o escopo da política: Apesar de não contemplar como documento final uma PSI completa e finalizada, o resultado final apresentado aqui, tem por princípio desenhar o escopo da política uma vez que as respostas ao questionário proporcionaram as bases para consolidação da mesma na ies.

Acredita-se que política será eficiente, pois ela é genuína e de simples entendimento para as áreas em que serão aplicadas. Faz-se necessário ainda, consolidar os processos e fluxos da informação na instituição segundo os resultados do questionário para assim descrevê-los e desenhar com maior profundidade a política em sua versão final.

É importante destacar que a falta da política de segurança da informação na ies desencadeia problemas de natureza simples e potencializa situações que são hoje são facilmente resolvidas com ações simples de segurança da informação como backups periódicos e armazenamento adequado, reuniões e instruções sobre questões básicas de segurança da informação com os funcionários, pois para o usuário executar suas tarefas com eficácia no dia a dia é necessário que ele se sinta confortável e seguro no ambiente que ele opera suas atividades.

Uma instituição que segue normas de segurança reconhecidas mundialmente como as que foram citadas ao longo do trabalho, geralmente obtêm um nível de excelência maior que as instituições que não seguem, caracterizando obviamente um fator que aumenta a credibilidade do negócio.

A segurança da informação só será obtida se as regras estabelecidas forem cumpridas e isso exige uma postura profissional das pessoas envolvidas no negócio.

A informação dentro da instituição só deve ser liberada para quem realmente necessita dela para realizar suas atividades no dia a dia.

O objetivo deste trabalho foi alcançado tendo em vista que a PSI foi elaborada a partir dos resultados obtidos com o questionário e o setor administrativo atendido pela mesma como aquele que carecia de urgência no estabelecimento de diretrizes para segurança da informação.

Como recomendações para estudos futuros, destaca-se a necessidade de continuidade da PSI e implantação efetiva na IES.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS ISO/IEC 27001:2006. **Sistema de gestão de segurança da informação**. Disponível em: <http://www.renatodacosta.net/27001.pdf>. Acesso em: 01 ago. 2017.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 27002:2005. **Código de prática para a gestão da segurança da informação**. Disponível em <http://newmoro.blogspot.com/2010/07/nbr-iso-27002-para-download.html>. Acesso em: 09 ago. 2017.

Avast – **Vírus de Computador**. Disponível em: <https://www.avast.com/pt-br/c-computer-virus>. Acesso em 06 de nov. 2017.

CASTILHO, Sérgio Duque; FONTE, Miguel Feitoza. **Política de Segurança da Informação Aplicada em Uma Instituição de Ensino Mediante Análise de Risco**. Revista da FATEC OURINHOS, São Paulo, n. 2, p. 51-66, 2012.

DANCHEV, Dancho. **Building and Implementing a Successful information Security Policy.** Disponível em: <http://www.windowsecurity.com/pages/security-policy.pdf>. Acessado em: 09 ago. 2017.

ENSSLIN, Leonardo; VIANNA, William Barbosa. O design na pesquisa quali-quantitativa em engenharia de produção–questões epistemológicas. **Revista Produção Online**, v. 8, n. 1, 2008. Disponível em: <https://scholar.google.com.br/scholar?hl=pt-BR&as_sdt=0%2C5&q=quali-quantitativa&btnG=>. Acesso em: 03 nov. 2017.

FERREIRA, Fernando N.F. ; ARAÚJO, Márcio T. **Política de Segurança da Informação: Guia Prático para Elaboração e Implementação**. 2 ed. Rio de Janeiro: Editora Ciência Moderna Ltda, 2008.

FONTES, Edison Luiz Gonçalves. **Praticando a Segurança da Informação**. Rio de Janeiro: Brasport, 2008.

NBR/ISO/IEC 17799. **Tecnologia da Informação**: Código de prática para a gestão da segurança da informação. ABNT, 2005

LYRA, Maurício R. **Segurança e Auditoria em Sistemas de Informação**. Rio de Janeiro: Ciência Moderna, 2008.

OLIVEIRA, Wilson José de. **Segurança da Informação**. Florianópolis: Visual Books, Maio, 2001.

Portal Informativo – ISO 27001. Disponível em: <https://www.27001.pt>. Acesso em: 21 mar. 2017

SPANCESKI, Francini Reitz. 2004. **Política de Segurança da Informação – Desenvolvimento de um modelo voltado para instituições de ensino**. Disponível em: http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_francini_politicas.pdf. Acesso em: 10 mar. 2017.